What’s happening on campus?

CampusGuard to Visit Next Month

Ed Ko, our Qualified Security Assessor (QSA) from CampusGuard, will visit Binghamton University on July 25th and 26th. Departments that he will visit have been contacted individually to arrange a meeting. Most of the departments visited last year will not be revisited this year. During his visit, he will lead a discussion open to all about the PCI DSS. This will take place in the Admissions Center classroom (AM-189) on Monday, July 25th beginning at 8:45am. PLEASE NOTE: Attendance at this Monday morning session will count towards the annual training requirement. For those who need to complete training, you won’t have to take the computer based module. We will also discuss point to point encryption at this session, where we plan to deploy it on campus, and how it will help us achieve PCI compliance.

PCI DSS Compliance Training 2016

More than 200 employees have completed training thus far. Thanks to all of you who have done so. However, 95 still need to complete the required training. To do so, please visit the following web site and follow the instructions:

http://www.binghamton.edu/revenue-accounting/pci_dss/training.html

Alternatively, you can attend the session mentioned above led by Ed Ko. This will excuse you from computer based training.

Remember, Binghamton University cannot achieve PCI compliance unless everyone is properly trained on an annual basis. So your cooperation in this endeavor is greatly appreciated.

Did you know?

The University of Calgary in Alberta paid a ransom of $20,000 to decrypt their computer system files and regain access to their own email system after getting hit by a ransomware infection. The infection was initially caused by malware.

If you have credit card terminals at your office, please see the EMV Update on page two.
Outstanding Compliance Issues

1. Annual Training - there are still about 95 employees that need to complete training. Please ensure that everyone in your department is trained. Reminders will be sent out and continue until training is completed.

2. Many Attestations of Compliance (AOCs) from third parties have expired, and a few have never been obtained. If a third party collects payments on our behalf, we must ensure that company is PCI compliant
In addition, all contracts with third parties must contain PCI language. The proper language will make it easier to obtain the annual AOC.

If you have questions, please contact Steve Duseau. sduseau@binghamton.edu

Alert Regarding the Orlando Shootings

Cyber criminals are trying to benefit from the Orlando shootings. They are now sending out phishing campaigns that try to trick you into clicking on a variety of links about blood drives, charitable donations, "inside" information or "exclusive" videos. Don't let them shock you into clicking on anything, or open possibly dangerous attachments you did not ask for!

Anything you receive about the Orlando shootings, be very suspicious. With this topic, think three times before you click.

It is very possible that it is a scam, even though it might look legit or was forwarded to you by a friend -- be especially careful when it seems to come from someone you know through email, a text or social media postings because their account may be hacked.

In case you want to donate to charity, go to your usual charity by typing their name in the address bar of your browser and do not click on a link in any email. Remember, these precautions are just as important at the house as in the office, and tell your family.

Binghamton University EMV Update

We have now deployed credit card terminals capable of processing EMV chip cards at all campus merchant departments that use machines issued by M&T Bank. It was a long wait for the units that communicate via wireless cellular, but we now have them. Some campus merchants have payment processing integrated with their point of sale software. For those departments the software vendor, not M&T Bank, is responsible for providing EMV compliant terminals. So to some extent, the university is waiting on each individual software vendor to provide a solution that we can agree to.

Security Issue

During this terminal swap out process, an important security issue came to light. Our terminals from M&T all process credit cards via First Data Merchant Services (FDMS). This means that each machine contains a software download provided by First Data. Ed Ko of CampusGuard has informed us that the First Data software contains an administrative level, well known, default password that cannot be changed. If a machine was lost or stolen, it could be easily hacked using the default password. This makes the physical security of each credit card terminal extremely important. Please ensure that these machines are safeguarded by PCI trained employees during business hours. When your offices are closed, please store these machines in a locked cabinet within a locked office. If your office has a safe, please use it to store your credit card terminals.